

RECEIVED

JAN 27 2006

Technology Center 2100

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPLICANT(s): Vanttinen et al.

SERIAL NO.: 09/864,017

ART UNIT: 2135

FILING DATE: 05/23/2001

EXAMINER: Truong

Thanhhoa

TITLE: METHOD FOR PROCESSING LOCATION INFORMATION  
RELATING TO A TERMINAL CONNECTED TO A PACKET  
NETWORK VIA A CELLULAR NETWORK

ATTORNEY

DOCKET NO.: 297-010337-US (PAR)

Board of Patent Appeals and Interferences  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450

**APPELLANTS' BRIEF**  
**(37 C.F.R. § 41.37)**

This is an appeal from the final rejection of the claims in the above-identified application. A Notice of Appeal was mailed on November 21, 2005. The fees required under 37 C.F.R. § 41.20 are being submitted herewith.

**I. REAL PARTY IN INTEREST**

The real party in interest in this Appeal is the Assignee, Nokia Mobile Phones Ltd., Espoo, Finland.

## **II. RELATED APPEALS AND INTERFERENCES**

There are no related appeals or interferences regarding this application.

## **III. STATUS OF CLAIMS**

Claims 1-34 are pending in the application.

Claims 1-34 have been finally rejected.

Claims 1-34 are on appeal.

## **IV. STATUS OF AMENDMENTS**

No amendments were made to the claims in response to the final rejection of the claims.

## **V. SUMMARY OF CLAIMED SUBJECT MATTER**

Claim 1 recites a method (Fig. 4) for processing location information, which is related to a certain mobile station in a cellular network. The method comprises a first network element, which is connected to the cellular network (P. 6, L. 28-30), receiving (Fig. 4, Ref. No. 401) a location information request (Fig. 2, Ref. No. 201) relating to the mobile station from a second network element, which is connected to a packet data network (P. 11, L. 20-29). Requesting (Fig. 4, Ref. No. 404)

from a third network element, which is connected to the packet data network, a security document relating to the second network element (P. 11, L. 29-32). Initiating the establishment (Fig. 4, Ref. No. 406) of at least one security association, which security association specifies at least data origin authentication and points from the second network element to the first network element and which establishment involves use of information comprised in the security document (P. 11, L. 30-34; P. 12, L. 26 - P. 14, L. 14; Figs. 5 and 6). After successful establishment of said security association, authenticating (Fig. 4, Ref. No. 408) the data origin of the location service request (P. 12, L. 1-4). If the data origin of the location service request is authenticated successfully, initiating (Fig. 4, Ref. No. 410) a location procedure relating to the mobile station in the cellular network (P. 12, L. 4-6).

Claim 21 recites a network element (P. 17, L. 1-2; Fig. 9, Ref. No. 900) of a cellular network. The network element comprises means (Fig. 9, Ref. No. 910) for receiving from a packet data network a location information request relating to a certain mobile station (P. 17, L. 8-10). Means (Fig. 9, Ref. No. 920) for initiating a location procedure in the cellular network (P. 17, L. 10-11). Means (Fig. 9, Ref. No. 930) for establishing security associations pointing to the network element from a network element of the packet data network (P. 17, L. 11-12). Means (Fig. 9, Ref. No. 931) for performing security functions as specified by the security associations on data it receives from the packet data network (P. 17, L. 14-16). Means (Fig. 9, Ref. No. 932) which are arranged to determine, if there is an existing security association pointing to the network element from a sender of a location information request (P. 17, L. 18).

Means (Fig. 9, Ref. No. 933) for initiating security association establishment, which are arranged to establish a security association if there does not exist a security association, which points towards the network element from the sender of a location information request (P. 17, L. 18-21).

Claim 27 recites a packet data device (Fig. 9, Ref. No. 950) being an integral part of a mobile station or being attachable to a mobile station (P. 17, L. 1-4; P. 18, L. 4-5). The packet data device comprises means (Fig. 9, Ref. No. 960) for receiving information about a location information request and about a sender of a location information request from a mobile station (P. 18, L. 6-8). Means (Fig. 9, Ref. No. 970) for exchanging with a network element connected to a cellular network information about a security association, which points to the network element from the sender of the location information request (P. 18, L. 8-11).

Claim 33 recites a mobile station comprising means for receiving a notification from a cellular network about a location information request (p. 18, L. 27-28). Means for responding to the cellular network with a notification response (P. 18, L. 28-29). Means for notifying a packet data device, which is either an integral part of the mobile station or attached to the mobile station, about the location information request (P. 18, L. 29-30).

## **VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

The issues presented for review are whether:

- A. claims 33-34 are patentable under 35 U.S.C. 102(e) over Jokiaho et al., U.S. Patent No. 5,889,770 ("Jokiaho");
- B. claims 1-5, 7 and 9-26 are patentable under 35 U.S.C. 103(a) over Havinis et al., U.S. Patent No. 6,671,377 ("Havinis"), in view of Jokiaho; and
- C. claims 6, 8 and 27-32 are patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiaho and in further view of Barnes et al., U.S. Patent No. 6,711,147 ("Barnes").

## **VII. ARGUMENT**

### **A. 35 U.S.C. 102(e)**

#### **1. Claim 33**

Claim 33 is patentable under 35 U.S.C. 102(e) over Jokiaho. Claim 33 of the present Application recites a mobile station, comprising means for receiving a notification from a cellular network about the location information request and means for notifying a packet data device, which is either an integral part of the mobile station or attached to the mobile station, about the location information request. Jokiaho fails to disclose or suggest these features.

Jokiaho discloses a GSM cellular radio system that is divided into radio cells. Base station systems are connected to a

mobile services switching center by digital transmission links (9) (Col. 4, L. 41-46). A data service center (19) is a process or computer (Col. 4, L. 62-63) and is connected to the mobile services switching center (10), a base station controller or a base station (Col. 5, L. 2-5). Data on the location of the mobile station of Jokiahio is maintained in a subscriber database in accordance with the location area configuration determined in the network (Col. 6, L. 27-31). The cellular network knows the location of the mobile stations with an accuracy of a larger area consisting of several cells (i.e. the location area) (Col. 6, L. 38-41). The mobile station registered in a cell knows which location area the base station belongs to on the basis of the location area identifier broadcast by the base station. When the mobile station moves from one cell to another the mobile station initiates location updating by transmitting a location updating request to the cellular radio network (Col. 6, L. 48-60). This request causes the subscriber information of the mobile station to be updated in the subscriber database of the cellular radio network (Col. 6, L. 61-63).

Jokiahio does not disclose or suggest a mobile station having means for receiving a notification from a cellular network about the location information request and means for notifying a packet data device, which is either an integral part of the mobile station or attached to the mobile station, about the location information request.

In Jokiahio, the mobile station initiates a location updating request only when the mobile station crosses a boundary between two cells (Col. 7, L. 19-24; Col. 7, L. 61-66). This is not the same as a "means for receiving a notification from a cellular

network about the location information request" as recited in claim 33. The mobile station of Jokiahho is not receiving a notification of any kind but rather is telling the cell radio network that it is moving from one cell to another. There is simply no disclosure or suggestion of a notification of a location information request being sent to the mobile station by the cell radio network. The mobile station in Jokiahho does initiate a location updating request to the cell radio network but this updating request is not the same as a means for receiving a notification from a cellular network about the location information request. The updating request of Jokiahho is unsolicited in that it is not requested by the network and merely tells the network that the mobile station is switching from one cell to another cell.

Furthermore, there is no disclosure whatsoever in Jokiahho of the mobile station having a packet data device, which is either an integral part of the mobile station or attached to the mobile station.

The Examiner suggests that these features are met at column 3, lines 57-67 through column 4, lines 1-5 of Jokiahho. The Appellant disagrees. Column 3, line 57 through column 4, line 5 merely discloses that the location updating request sent to the service center by the mobile station can be augmented with the cell identifier of the cell or group of cells from which the mobile station transmitted them. This merely serves to provide a comparison with the previous cell identifier associated with the mobile station that was stored in the data service database. If the new cell identifier is different that the stored

identifier, the stored identifier is replaced with the new identifier.

This passage from Jokiaho essentially introduces a method with which location information travels as a constant stream from the terminal or mobile station to a network element without anyone requesting that location information. Appellant explicitly recites "receiving a notification from a cellular network about the location information request". In Jokiaho a request is not made to the mobile terminal (or the mobile communication network, in case it is the mobile communication network that inserts the cell identifiers according to column 4, lines 1-5) to insert the cell identifiers into the data packet, but rather the cell identifier's inclusion in the data packet is completely unsolicited. The inclusion of the cell identifiers in Jokiaho are not the same as a "notification from a cellular network about a location information request" or a "notification to a packet data device, which is either an integral part of the mobile station or attached to it, about the location information request" as called for in claim 33. There is simply no location information request made in Jokiaho.

Furthermore, it is unclear as to whether the Examiner is equating Jokiaho's "data service center" to the Appellant's "packet data device, which is either an integral part of the mobile station or attached to it". In any case, the data service center of Jokiaho is not the same as the packet data device of claim 33. In Jokiaho, the data service center is a computer located somewhere in the depths of a communications network. Thus, it cannot be an integral part of a mobile station or attached to the mobile station. In addition, the



data service center (19) is disclosed in Jokiahho as being connected to the mobile services switching center (10), a base station controller or a base station (Col. 5, L. 2-5). Thus, the data service center of Jokiahho is not connected to a mobile station, as recited by Appellant in claim 33. Thus, the data service center cannot be a data packet device as called for in claim 33.

Therefore, claim 33 is patentable over Jokiahho under 35 U.S.C. 102(e).

## 2. Claim 34

Claim 34 is dependent on claim 33 and is patentable under 35 U.S.C. 102(e) over Jokiahho at least for the reasons noted above with respect to claim 33. Further, claim 34 recites, the means for responding to the cellular network are arranged to be initiated by a permission sent by the packet data device.

As discussed above, there is no disclosure or suggestion of a data packet device in Jokiahho that is either an integral part of the mobile station or attached to the mobile station. The data service center (19) of Jokiahho cannot be a data packet device as recited in claim 34. In Jokiahho, the data service center is a computer located somewhere in the depths of a communications network. Thus, it cannot be an integral part of a mobile station or attached to the mobile station. In addition, the data service center (19) is disclosed in Jokiahho as being connected to a mobile services switching center (10), a base station controller or a base station (Col. 5, L. 2-5). Thus, In addition, Jokiahho can not disclose or suggest of a permission sent by the packet data device.

Moreover, in Jokiaho it is the cell radio network that responds to the mobile station's location updating request. Jokiaho discloses that location management system may comprise a location updating acknowledgement transmitted by the data service center (19). If the mobile station does not receive the acknowledgment, it repeats the location updating (Col. 9, L. 20-25). Claim 34 recites "responding to the cellular network", not responding to the mobile station. Therefore, claim 34 is patentable over Jokiaho.

B. 35 U.S.C. 103(a)

1. Claim 1

Claim 1 is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiaho. Claim 1 recites a first network element receiving a location information request from a second network element, requesting from a third network element a security document relating to the second network element and initiating the establishment of at least one security association that specifies data origin authentication and points from the second network element to the first network element. These features are not disclosed or suggested by Havinis in view of Jokiaho.

Havinis discloses a telecommunications system and method for downloading encrypted network information, such as base transceiver station coordinates between the network and the mobile station (Col. 3, L. 15-20). When the mobile station (20) performs a location calculation the mobile station (20) does not need to involve the network (10) in the positioning process except to obtain access to network information, e.g. base

transceiver station (24) coordinate information. The base transceiver coordinate information is obtained by the mobile station sending a mobile originating request for assistance data (215). This mobile originating request for assistance data (215) requests from the network (10) a location deciphering key and includes a positioning indication (218) that indicates to the network (10) the number and/or duration of the positionings that the mobile station (20) will be performing (Col. 5, L. 32-44). In response to a mobile originating request for assistance data (215), the mobile switching center (14) sends a security related information request (219), which includes the positioning indication (218), to a home location register (26) associated with the mobile station (20) (Col. 5, L. 45-50). Encrypted network information (320) is transmitted to the mobile station (20) over a broadcast control channel (21) (Col. 5, L. 60-62). This is not what is claimed in Appellant's claim 1.

The Examiner cites to column 4, lines 30-47 and column 5, lines 37-62 in making the rejection of claim 1. In Havinis, the serving mobile location center receives a positioning request for a particular target mobile station (20) (Col. 4, L. 30-36). The serving mobile location center can opt to allow the mobile station (20) to both obtain positioning measurements and to calculate it's own location based upon those position measurements (col. 5, L. 24-27). When the mobile station performs its own location calculations, it receives encrypted network information (e.g. the base transceiver station coordinate data). This however, is not what is recited in claim 1. Claim 1 recites a first network element receiving a location information request from a second network element and requesting from a third network element a security document. In the

Examiner's analysis the serving mobile location center receives the location request from an unknown party. Also in the Examiner's analysis the mobile station of Havinis requests the network information from the mobile switching center. This would mean that the first network element is the serving mobile location center, the second network element is the unknown party and the third network element is the mobile switching center. Claim 1 further recites "the security document relating to the second network element". In the Examiner's argument the location deciphering key at column 5, lines 37-44 is the security document, however the location deciphering key does not relate to the unknown party. The location deciphering key relates to the mobile station and its calculation of its position (Col. 5, L. 37-62).

Furthermore, claim 1 recites "initiating the establishment of at least one security association that specifies data origin authentication and points from the second network element to the first network element". Nowhere does Havinis disclose a security association that specifies data origin authentication and points from the second network element to the first network element. Havinis merely discloses a network that uses encryption algorithms. There are no dedicated security connections in Havinis nonetheless security associations that point from one network element to another network element. In addition, in the Examiner's analysis, as described above, the security association would have to point from the unknown party to the serving mobile location center. This is not the case in Havinis. Havinis merely discloses encryption between the mobile station and the mobile switching center. Nowhere does Havinis disclose any security association between the serving mobile

location center and the unknown party nonetheless a "pointing" security association as recited in claim 1. Havinis merely discloses the serving mobile location center receiving a positioning request [from the unknown party] (Col. 4, L. 30-36). Therefore, claim 1 is patentable over Havinis.

Jokiaho also fails to disclose or suggest the features of claim 1. Jokiaho discloses a GSM cellular radio system. In the cellular radio system, the area covered by the system is divided into radio cells (Col. 4, L. 41 - 43; Fig. 1). Packets from all mobile stations within a specified area are routed to the data service center (Col. 5, L. 7 - 9). Jokiaho simply does not disclose or suggest "requesting a security document" and "initiating the establishment of at least one security association that specifies data origin authentication and points from the second network element to the first network element" as recited in claim 1. Therefore, claim 1 is patentable over the combination of Havinis and Jokiaho for at least this reason.

Furthermore, the Examiner notes that Havinis fails to disclose that the second network element connects to a packet data network. The Examiner suggests that Jokiaho discloses this. However, there is no motivation to combine Havinis with Jokiaho to achieve Appellant's invention. In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must

teach or suggest all of the claim limitations (See M.P.E.P. § 2142).

As described above, Havinis does not disclose or suggest each feature of Appellant's invention as claimed. In addition, the object of Havinis is to download encrypted network information such as, base transceiver station coordinates, in a point-to-point manner between the network and the mobile station with location calculation capabilities (so the mobile station can calculate its location) (Col. 3, L. 15-20). Havinis is not at all concerned with who may and who may not access the location information of a mobile station. Havinis' only concern is how to send necessary information to a mobile station so the mobile station can use that information to calculate its location. Similarly, Jokiahho is not concerned with who may or may not access the location information of the mobile station. The object of Jokiahho is to reduce the amount of signaling for location management concerning packet transmission compared to location management concerning normal traffic (Abstract; Col. 3, L. 20-56). If Havinis and Jokiahho were combined the result would be a cellular network where the mobile station downloads base transceiver station coordinates so the mobile station can calculate its location in such a way to reduce the amount of signaling for location management of the mobile station.

Therefore, the references themselves and/or the knowledge generally available to one of skill in the art do not provide the requisite motivation or suggestion to modify the references as proposed for purposes of 35 U.S.C. 103(a). Neither reference, individually or in combination, discloses or suggests limiting access to the location information of the mobile

station by "initiating the establishment of at least one security association, which security association specifies at least data origin authentication and points from the second network element to the first network element and which establishment involves use of information comprised in the security document" and "authenticating the data origin of the location service request" as called for in claim 1.

Claims 2-5, 7 and 9-20 are patentable under 35 U.S.C. 103(a) at least by reason of their respective dependencies over Havinis in view of Jokiahho.

## 2. Claim 2

Claim 2 is dependent on claim 1 and is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiahho at least for the reasons noted above with respect to claim 1. Further, claim 2 recites, the security document relating to the second network element is a public key certificate, which comprises an identifier specifying the second network element and a public key of the second network element and which is cryptographically signed by the third network element. Neither Havinis nor Jokiahho, individually or in combination, disclose or suggest these features.

In the Examiner's analysis, the first network element is the serving mobile location center, the second network element is the unknown party and the third network element is the mobile switching center. Havinis discloses a location deciphering key at column 5, lines 37-44, however the location deciphering key does not relate to the unknown party. The location deciphering

key relates to the mobile station and its calculation of its position (Col. 5, L. 37-62). Havinis also discloses a subscriber identification key at column 5, lines 50-58 but this subscriber identification key relates to the mobile station and not the unknown party. Therefore, neither the subscriber identification key nor the location deciphering key can be a security document relating to the second network element. Moreover, Havinis does not disclose that the subscriber identification key or the location deciphering key are signed by mobile switching station.

Jokiaho merely discloses that "at the registration stage, there is also an exchange of ciphering keys which are used in the packets transmitted subsequently" (Col. 7, L. 56-58). Jokiaho simply does not disclose or suggest the security document relating to the second network element is a public key certificate, which comprises an identifier specifying the second network element and a public key of the second network element and which is cryptographically signed by the third network element.

In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). As described above, both Havinis and Jokiaho fail to disclose or suggest the security document relating to the second network element is a



public key certificate, which comprises an identifier specifying the second network element and a public key of the second network element and which is cryptographically signed by the third network element as recited in claim 2. Therefore, claim 2 is patentable over Havinis and/or Jokiahho, individually or in combination, because neither reference discloses or suggests all the features of claim 2.

### 3. Claim 3

Claim 3 is dependent on claim 1 and is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiahho at least for the reasons noted above with respect to claim 1. Further, claim 3 recites, requesting from the third network element a second security document relating to the first network element. Neither Havinis nor Jokiahho, individually or in combination, disclose or suggest these features.

Havinis discloses a location deciphering key at column 5, lines 37-44 and a subscriber identification key at column 5, lines 50-58. Both the location deciphering key and the subscriber identification key relate to the mobile station and its calculation of its position (Col. 5, L. 37-62). Havinis does not disclose or suggest requesting a security document or key from the mobile switching center (i.e. the third network element in the Examiner's analysis) relating to the serving mobile location center (i.e. the first network element in the Examiner's analysis). Therefore, neither the subscriber identification key nor the location deciphering key can be the second security document relating to the first network element.

Jokiaho merely discloses that "at the registration stage, there is also an exchange of ciphering keys which are used in the packets transmitted subsequently" (Col. 7, L. 56-58).

In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). As described above, neither Havinis nor Jokiaho disclose or suggest a second security document relating to the first network element. Therefore, claim 3 is patentable over Havinis and/or Jokiaho, individually or in combination, because neither reference discloses or suggests all the features of claim 3.

#### 4. Claim 4

Claim 4 is ultimately dependent on claim 1 and is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiaho at least for the reasons noted above with respect to claim 1. Further, claim 4 recites, the security document comprises a first key, which is encrypted using a second key shared between the first network element and the third network element, and the second security document comprises the first key, which is encrypted using a third key shared between the second network element and the third network element. Neither Havinis nor Jokiaho, individually or in combination, disclose or suggest these features.

Havinis discloses a location deciphering key at column 5, lines 37-44 and a subscriber identification key at column 5, lines 50-58, both of which relate to the mobile station and its calculation of its position (Col. 5, L. 37-62). The mobile station (20) requests from the network (10) the location deciphering key. The AuC (27) fetches the subscriber identification key stored within a subscriber record (29) associated with the mobile station (20) from the HLR (26) and uses this identification key together with a non-predictable random number and the positioning indication (218), which indicates the number of positioning requests, as an input to a ciphering algorithm (28), which corresponds to the deciphering algorithm (255) supported by the mobile station (20), to derive the location deciphering key. The location deciphering key is sent back to the mobile switching center (14) for use by the BSC (232) in encrypting the network information (Col. 5, L. 45-62). Neither of these keys is shared between the security mobile location center and the mobile switching center or the unknown party and the mobile switching center. Moreover, there are only two keys disclosed in Havinis (i.e. the location deciphering key and the subscriber identification key. A subscriber identity key is disclosed in claim 22, however there is no reference to a subscriber identity key in the specification and when the claim is construed according to the specification the subscriber identity key is the same as the subscriber identification key). Appellant's claim 4 recites a "third key". Therefore, Havinis fails to disclose the features of claim 4.

Jokiaho merely discloses that "at the registration stage, there is also an exchange of ciphering keys which are used in the packets transmitted subsequently" (Col. 7, L. 56-58).

In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). For the reasons described above, neither Havinis nor Jokiahho disclose or suggest the security document comprises a first key, which is encrypted using a second key shared between the first network element and the third network element, and the second security document comprises the first key, which is encrypted using a third key shared between the second network element and the third network element. Therefore, claim 4 is patentable over Havinis and/or Jokiahho, individually or in combination, because neither reference discloses or suggests the features of claim 4.

#### 5. Claim 5

Claim 5 is ultimately dependent on claim 1 and is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiahho at least for the reasons noted above with respect to claim 1. Further, claim 5 recites, initiating the establishment of a second security association from the first network element to the second network element using at least information comprised in the second security document. Neither Havinis nor Jokiahho, individually or in combination, disclose or suggest these features.

Havinis discloses a location deciphering key at column 5, lines 37-44 and a subscriber identification key at column 5, lines 50-58, neither of which are used in the communication between the serving mobile location center and the unknown party. Both of these keys relate to the mobile station and its calculation of its position (Col. 5, L. 37-62). Havinis merely discloses that when a positioning request for a particular mobile station is received by a serving mobile location center serving a cell within the public land mobile network that the mobile station is currently located in, the servicing mobile station must choose the optimum position method available (e.g. timing advance, time of arrival, angle of arrival, GPS, etc.) (Col. 4, L. 30-47). Therefore, Havinis does not disclose a second security association from the first network element to the second network element using at least information comprised in the second security document.

Jokiaho also fails to disclose the features of claim 5. Jokiaho merely discloses that "at the registration stage, there is also an exchange of ciphering keys which are used in the packets transmitted subsequently" (Col. 7, L. 56-58).

In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). Neither Havinis nor Jokiaho discloses a second security association from the first

network element to the second network element using at least information comprised in the second security document for the reasons noted above. Therefore, claim 5 is patentable over Havinis and/or Jokiahho, individually or in combination, because neither reference discloses or suggests the features of claim 5.

#### 6. Claim 9

Claim 9 is dependent on claim 1 and is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiahho at least for the reasons noted above with respect to claim 1. Further, claim 9 recites, establishing at least one security association, which specifies at least data origin authentication and which points from the second network element to the first network element, using at least information comprised in the security document and after the establishment of the security association, authenticating the data origin at the location service request. Neither Havinis nor Jokiahho, individually or in combination, disclose or suggest these features.

Havinis discloses that when a positioning request (generated by an unknown party, i.e. the second network element in the Examiner's analysis) for a particular mobile station is received by a serving mobile location center (i.e. the first network element in the Examiner's analysis) serving a cell within the public land mobile network that the mobile station is currently located in, the serving mobile location center must choose the optimum position method available (e.g. timing advance, time of arrival, angle of arrival, GPS, etc.) (Col. 4, L. 30-47). There is no disclosure or suggestion in Havinis that "at least one security association, which specifies at least data origin

authentication and which points from the second network element to the first network element, using at least information comprised in the security document" is established between the unknown party and the serving mobile location center. In addition, Havinis does not disclose or suggest "authenticating the data origin at the location service request". Havinis merely mentions that a location request is received by the serving mobile location center. Therefore, claim 9 is patentable over Havinis.

In Jokiahö, the mobile station initiates a location updating request only when the mobile station crosses a boundary between two cells (Col. 7, L. 19-24; Col. 7, L. 61-66). There is simply no location information request disclosed or suggested in Jokiahö. The location updating request is not a request for information but rather tells the cellular radio network to update the subscriber information of the mobile station in the subscriber database of the cellular radio network with respect to which cell the mobile station is located (Col. 6, L. 27-63). Jokiahö is only concerned with diminishing the extra signalling caused by location updating by providing the data packets arriving at the data service center from a mobile station with the identifier of the cell or group of cells from which the mobile station transmitted them (Col. 3, L. 57-61). Further, Jokiahö does not disclose "using at least information comprised in the security document" as recited in claim 9. Jokiahö merely recites that at the registration stage, there is also an exchange of ciphering keys which are used in the packets transmitted subsequently (Col. 7, L. 56-58). Thus, Jokiahö does not disclose or suggest at least data origin authentication and which points from the second network element to the first

network element, using at least information comprised in the security document.

In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). Neither Havinis nor Jokiaho disclose or suggest establishing at least one security association, which specifies at least data origin authentication and which points from the second network element to the first network element, using at least information comprised in the security document and after the establishment of the security association, authenticating the data origin at the location service request as described above. Therefore, claim 9 is patentable over the combination of Havinis and Jokiaho.

#### 7. Claim 12

Claim 12 is ultimately dependent on claim 1 and is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiaho at least for the reasons noted above with respect to claim 1. Further, claim 12 recites, establishing a second security association, which specifies at least data encryption and points from the first network element to the second network element, using at least the information specified in the second security document. Neither Havinis nor Jokiaho, individually or in combination, disclose or suggest these features.



As described above, Havinis discloses that when a positioning request (generated by an unknown party, i.e. the second network element in the Examiner's analysis) for a particular mobile station is received by a serving mobile location center (i.e. the first network element in the Examiner's analysis) serving a cell within the public land mobile network that the mobile station is currently located in, the serving mobile location center must choose the optimum position method available (e.g. timing advance, time of arrival, angle of arrival, GPS, etc.) (Col. 4, L. 30-47). Havinis does not disclose or suggest a second security association, which specifies at least data encryption and points from the first network element to the second network element, using at least the information specified in the second security document. Havinis merely mentions that a location request is received by the serving mobile location center. Therefore, claim 12 is patentable over Havinis.

Jokiaho, also fails to disclose the features of claim 12. Jokiaho is only concerned with diminishing the extra signalling caused by location updating by providing the data packets arriving at the data service center from a mobile station with the identifier of the cell or group of cells from which the mobile station transmitted them (Col. 3, L. 57-61). Further, Jokiaho does not disclose "using at least information comprised in the second security document" as recited in claim 12. Jokiaho merely recites that at the registration stage, there is also an exchange of ciphering keys which are used in the packets transmitted subsequently (Col. 7, L. 56-58).

In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation,

whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). Neither Havinis nor Jokiahho disclose or suggest establishing a second security association, which specifies at least data encryption and points from the first network element to the second network element, using at least the information specified in the second security document. Therefore, claim 12 is patentable over the combination of Havinis and Jokiahho.

#### 8. Claim 13

Claim 13 is ultimately dependent on claim 1 and is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiahho at least for the reasons noted above with respect to claim 1. Further, claim 13 recites, before transmitting the location information to the second network element, establishing a third security association, which specifies at least data origin authentication and points from the second network element to a packet data device, which is either connected to the mobile station or is an integral part of the mobile station. Neither Havinis nor Jokiahho, individually or in combination disclose these features.

The Examiner notes that Havinis fails to disclose that the second network element connects to a packet data network. Therefore, Havinis can not disclose a data packet device being either connected to the mobile station or is an integral part of the mobile station as recited in claim 13 as evidenced by the

figures of Havinis (Figs. 1, 2, 3, 4A, 5, 7 and 9). Further, Havinis does not disclose or suggest "data origin authentication" as claimed in claim 13. Havinis discloses that when a positioning request (generated by an unknown party, i.e. the second network element in the Examiner's analysis) for a particular mobile station is received by a serving mobile location center (i.e. the first network element in the Examiner's analysis) serving a cell within the public land mobile network that the mobile station is currently located in, the serving mobile location center must choose the optimum position method available (e.g. timing advance, time of arrival, angle of arrival, GPS, etc.) (Col. 4, L. 30-47). There is simply no disclosure or suggestion in Havinis of "establishing a third security association, which specifies at least data origin authentication" as Havinis merely mentions that a location request is received by the serving mobile location center.

Jokiaho also fails to disclose or suggest the features of claim 13. In Jokiaho, the mobile station initiates a location updating request only when the mobile station crosses a boundary between two cells (Col. 7, L. 19-24; Col. 7, L. 61-66). Furthermore, there is no disclosure whatsoever in Jokiaho of the mobile station having a packet data device, which is either an integral part of the mobile station or attached to the mobile station. Jokiaho discloses that the location updating request sent to the data service center by the mobile station can be augmented with the cell identifier of the cell or group of cells from which the mobile station transmitted them. This merely serves to provide a comparison with the previous cell identifier associated with the mobile station that was stored in the data service database. If the new cell identifier is different that

the stored identifier, the stored identifier is replaced with the new identifier. The data service center of Jokiahho is not the same as the packet data device of claim 13 as the data service center of Jokiahho is a computer located somewhere in the depths of a communications network and cannot be an integral part of a mobile station or attached to the mobile station. In addition, the data service center (19) is disclosed in Jokiahho as being connected to a data service center (19) to the mobile services switching center (10), a base station controller or a base station (Col. 5, L. 2-5).

In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations. (See M.P.E.P. § 2142). As described above, neither Havinis nor Jokiahho disclose or suggest establishing a third security association, which specifies at least data origin authentication and points from the second network element to a packet data device, which is either connected to the mobile station or is an integral part of the mobile station. Therefore, claim 13 is patentable over Havinis and/or Jokiahho, individually or in combination, because neither reference discloses or suggests the features of claim 13.

9. Claim 15

Claim 15 is ultimately dependent on claim 1 and is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiahho at least for the reasons noted above with respect to claim 1. Further, claim 15 recites, establishing a third security association, which specifies at least data origin authentication and points from the second network element to a packet data device, which is either connected to the mobile station or an integral part of the mobile station. Neither Havinis nor Jokiahho, individually or in combination disclose these features.

The Examiner notes that Havinis fails to disclose that the second network element connects to a packet data network. Therefore, Havinis can not disclose a data packet device being either connected to the mobile station or is an integral part of the mobile station as recited in claim 13 as evidenced by the figures of Havinis (Figs. 1, 2, 3, 4A, 5, 7 and 9). Further, Havinis does not disclose or suggest "data origin authentication" as claimed in claim 15. Havinis discloses that when a positioning request (generated by an unknown party, i.e. the second network element in the Examiner's analysis) for a particular mobile station is received by a serving mobile location center (i.e. the first network element in the Examiner's analysis) serving a cell within the public land mobile network that the mobile station is currently located in, the serving mobile location center must choose the optimum position method available (e.g. timing advance, time of arrival, angle of arrival, GPS, etc.) (Col. 4, L. 30-47). There is simply no disclosure or suggestion in Havinis of "establishing a third security association, which specifies at least data origin

authentication" as Havinis merely mentions that a location request is received by the serving mobile location center.

Jokiaho also fails to disclose or suggest the features of claim 15. In Jokiaho, the mobile station initiates a location updating request only when the mobile station crosses a boundary between two cells (Col. 7, L. 19-24; Col. 7, L. 61-66). Furthermore, there is no disclosure whatsoever in Jokiaho of the mobile station having a packet data device, which is either an integral part of the mobile station or attached to the mobile station. Jokiaho discloses that the location updating request sent to the data service center by the mobile station can be augmented with the cell identifier of the cell or group of cells from which the mobile station transmitted them. This merely serves to provide a comparison with the previous cell identifier associated with the mobile station that was stored in the data service database. If the new cell identifier is different than the stored identifier, the stored identifier is replaced with the new identifier. Also, the data service center of Jokiaho is not the same as the packet data device of claim 15 as the data service center of Jokiaho is a computer located somewhere in the depths of a communications network and cannot be an integral part of a mobile station or attached to the mobile station. In addition, the data service center (19) is disclosed in Jokiaho as being connected to a data service center (19) to the mobile services switching center (10), a base station controller or a base station (Col. 5, L. 2-5).

In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge

generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). Neither Havinis nor Jokiaho disclose or suggest establishing a third security association, which specifies at least data origin authentication and points from the second network element to a packet data device, which is either connected to the mobile station or an integral part of the mobile station as described above. Therefore, claim 15 is patentable over Havinis and/or Jokiaho, individually or in combination, because neither reference discloses or suggests the features of claim 15.

10. Claim 17

Claim 17, which depends from claim 9 and is ultimately dependent on claim 1 and is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiaho at least for the reasons noted above with respect to claim 1. Further, claim 17 recites, the mobile station receiving a notification relating to the location procedure relating to the mobile station and the mobile station informing said packet data device about the notification. Neither Havinis nor Jokiaho, individually or in combination, disclose or suggest these features.

Havinis does not disclose receiving a notification relating to the location procedure relating to the mobile station. Havinis merely discloses when a positioning request (285) for a particular target mobile station (20) is received by a serving mobile location center (270) serving cell (22) within the public

land mobile network (10) that the mobile station is currently located in the serving mobile location center (270) must choose the optimum positioning method available (col. 4, L. 30-36). Further, the only communication from the mobile station to the network (10) disclosed in Havinis is the mobile originating request for assistance data which requests from the network (10) a location deciphering key and includes a positioning indication (218) that indicates to the network (10) the number and/or duration of the positionings that the mobile station will be performing (Col. 5, L. 37-44). Thus, there is no disclosure of the mobile station in Havinis "informing said packet data device about the notification".

Further, in Jokiahho, the mobile station initiates a location updating request only when the mobile station crosses a boundary between two cells (Col. 7, L. 19-24; Col. 7, L. 61-66). This is not the same as a "the mobile station receiving a notification relating to the location procedure relating to the mobile station" as recited in claim 17. The mobile station of Jokiahho is not receiving a notification of any kind but rather is telling the cell radio network that it is moving from one cell to another. There is simply no disclosure or suggestion of "the mobile station receiving a notification relating to the location procedure relating to the mobile station and the mobile station informing said packet data device about the notification". The mobile station in Jokiahho does initiate a location updating request to the cell radio network but this updating request is not the same as receiving a notification relating to the location procedure relating to the mobile station. The updating request of Jokiahho is unsolicited in that it is not requested by the network and merely tells the network that the mobile station



is switching from one cell to another cell. Furthermore, there is no disclosure whatsoever in Jokiahho of the mobile station having a packet data device, which is either an integral part of the mobile station or attached to the mobile station.

In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). Neither Havinis nor Jokiahho disclose or suggest the mobile station receiving a notification relating to the location procedure relating to the mobile station and the mobile station informing said packet data device about the notification. Therefore, claim 17 is patentable over Havinis and/or Jokiahho, individually or in combination, because neither reference discloses or suggests the features of claim 17.

#### 11. Claim 21

Claim 21 is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiahho. Claim 21 recites means for establishing security associations pointing to the network element from a network element of the packet data network, means for performing security functions as specified by the security associations on data it receives from the packet data network, means which are arranged to determine, if there is an existing security association pointing to the network element from a sender of a

location information request, and means for initiating security association establishment, which are arranged to establish a security association if there does not exist a security association, which points towards the network element from the sender of a location information request. Havinis and Jokiahio fail to disclose or suggest these features.

Havinis discloses a telecommunications system and method for downloading encrypted network information, such as base transceiver station coordinates between the network and the mobile station (Col. 3, L. 15-20). When the mobile station (20) performs a location calculation the mobile station (20) does not need to involve the network (10) in the positioning process except to obtain access to network information, e.g. base transceiver station (24) coordinate information. The base transceiver coordinate information is obtained by the mobile station sending a mobile originating request for assistance data (215). This mobile originating request for assistance data (215) requests from the network (10) a location deciphering key and includes a positioning indication (218) that indicates to the network (10) the number and/or duration of the positionings that the mobile station (20) will be performing (Col. 5, L. 32-44). In response to a mobile originating request for assistance data (215), the mobile switching center (14) sends a security related information request (219), which includes the positioning indication (218), to a home location register (26) associated with the mobile station (20) (Col. 5, L. 45-50). Encrypted network information (320) is transmitted to the mobile station (20) over a broadcast control channel (21) (Col. 5, L. 60-62). This is not what is claimed in Appellant's claim 21.

In Havinis, the serving mobile location center receives a positioning request for a particular target mobile station (20) (Col. 4, L. 30-36). The serving mobile location center can opt to allow the mobile station (20) to both obtain positioning measurements and to calculate it's own location based upon those position measurements (col. 5, L. 24-27). When the mobile station performs its own location calculations, it receives encrypted network information (e.g. the base transceiver station coordinate data). This however, is not what is recited in claim 21. Claim 21 recites means for establishing security associations pointing to the network element from a network element of the packet data network, means for performing security functions as specified by the security associations on data it receives from the packet data network, means which are arranged to determine, if there is an existing security association pointing to the network element from a sender of a location information request, and means for initiating security association establishment, which are arranged to establish a security association if there does not exist a security association, which points towards the network element from the sender of a location information. Havinis merely discloses a network that uses encryption algorithms. There are no dedicated security connections in Havinis nonetheless security associations that point from one network element to another network element. Havinis merely discloses encryption between the mobile station and the mobile switching center. Nowhere does Havinis disclose any security association between the serving mobile location center and the unknown party (i.e. the sender of the location information request) nonetheless a "pointing" security association as recited in claim 21. Havinis merely discloses the serving mobile location center receiving a

positioning request [from the unknown party] (Col. 4, L. 30-36). Therefore, claim 21 is patentable over Havinis.

Jokiaho also fails to disclose or suggest the features of claim 21. Jokiaho discloses a GSM cellular radio system. In the cellular radio system, the area covered by the system is divided into radio cells (Col. 4, L. 41 - 43; Fig. 1). Packets from all mobile stations within a specified area are routed to the data service center (Col. 5, L. 7 - 9). The mobile station of Jokiaho initiates a location updating request only when the mobile station crosses a boundary between two cells (Col. 7, L. 19-24; Col. 7, L. 61-66). This location updating request causes the subscriber information of the mobile station to be updated in the subscriber database of the cellular radio network (Col. 6, L. 61-63). Jokiaho simply does not disclose or suggest "establishing security associations pointing to the network element from a network element of the packet data network" and a "security association pointing to the network element from a sender of a location information request" as recited in claim 21. Jokiaho merely discloses that at the registration stage [of the mobile station], there is also an exchange of ciphering keys which are used in the packets transmitted subsequently [to and from the mobile station] (Col. 7, L. 39-60). Therefore, claim 21 is patentable over the combination of Havinis and Jokiaho for at least this reason.

Furthermore, the Examiner notes that Havinis fails to disclose that the second network element connects to a packet data network. The Examiner suggests that Jokiaho discloses this. However, there is no motivation to combine Havinis with Jokiaho to achieve Appellant's invention. In order to establish a *prima*

*facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). As described above, Havinis and Jokiahho do not disclose or suggest each feature of Appellant's invention as claimed. Therefore, claim 21 is patentable over the combination of Havinis and Jokiahho.

C. 35 U.S.C. 103(a)

1. Claim 6

Claim 6 is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiahho in further view of Barnes. Claim 6 recites the security association is a set of Internet Security Associations pointing from the second network element to the first network element and the second security association is a second set of Internet Security Associations pointing from the first network element to the second network element. Neither Havinis, Jokiahho and Barnes discloses or suggests these features.

Havinis merely mentions a positioning request is received (from the unknown party, i.e. the second network element in the Examiner's analysis) by a serving mobile location center (i.e. the first network element in the Examiner's analysis) (Col. 4, L. 30-36) and does not disclose or suggest any type of security association between the unknown party and the serving mobile location center. Jokiahho discloses a cellular radio system

where the area covered by the system is divided into radio cells (Col. 4, L. 41 - 43; Fig. 1). Packets from all mobile station within a specified area are routed to the data service center (Col. 5, L. 7 - 9). Jokiahio simply does not disclose or suggest "a set of Internet Security Association pointing from the second network element to the first network element" as recited in claim 6.

Barnes discloses the merging of a GPRS network and a mobile internet protocol (Col. 4, L. 28-32). The GPRS network (200) includes a base station (16) that is connected to the servicing GPRS support node (30) through interface (32). The servicing GPRS support node (30) is connected to the gateway GPRS support node (40) through an intra PLMN backbone (204). The GPRS network also includes a border gateway (206). The mobile IP network (202) includes an intranet (104) with a home agent (106a) and one or more foreign agents (106b). A host (105) is located on the intranet (104) (Col. 6, L. 43-56). The GPRS network (250) connects to base station (16a, 16b) which are capable of establishing a wireless link with the mobile node (12) (Col. 7, L. 24-26). The IP Security and the security gateway of Barnes do not point to any one element of the network. IP security is merely a type of encryption while the security gateway is a firewall for protection against the outside world (Col. 6, L. 50-52). The IP Security and the security gateway are not disclosed as pointing from one network device to another. Nowhere does Barnes disclose or suggest "a set of Internet Security Association pointing from the second network element to the first network element".

In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). As described above, the combination of Havinis, Jokiahho and Barnes simply does not disclose or suggest the security association is a set of Internet Security Associations pointing from the second network element to the first network element and the second security association is a second set of Internet Security Associations pointing from the first network element to the second network element. Therefore, claim 6 is patentable over the combination of Havinis Jokiahho and Barnes.

## 2. Claim 8

Claim 8 is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiahho in further view of Barnes. Claim 8 recites the security association is a set of Internet Security Associations pointing from the second network element to the first network element. Neither Havinis, Jokiahho and Barnes discloses or suggests these features.

Havinis merely mentions a positioning request is received (from the unknown party, i.e. the second network element in the Examiner's analysis) by a serving mobile location center (i.e. the first network element in the Examiner's analysis) (Col. 4, L. 30-36) and does not disclose or suggest any type of security association between the unknown party and the serving mobile

location center. Jokiahho discloses a cellular radio system where the area covered by the system is divided into radio cells (Col. 4, L. 41 - 43; Fig. 1). Packets from all mobile station within a specified area are routed to the data service center (Col. 5, L. 7 - 9). Jokiahho simply does not disclose or suggest "a set of Internet Security Association pointing from the second network element to the first network element" as recited in claim 6.

Barnes discloses the merging of a GPRS network and a mobile internet protocol (Col. 4, L. 28-32). The GPRS network (200) includes a base station (16) that is connected to the servicing GPRS support node (30) through interface (32). The servicing GPRS support node (30) is connected to the gateway GPRS support node (40) through an intra PLMN backbone (204). The GPRS network also includes a border gateway (206). The mobile IP network (202) includes an intranet (104) with a home agent (106a) and one or more foreign agents (106b). A host (105) is located on the intranet (104) (Col. 6, L. 43-56). The GPRS network (250) connects to base station (16a, 16b) which are capable of establishing a wireless link with the mobile node (12) (Col. 7, L. 24-26). The IP Security and the security gateway of Barnes do not point to any one element of the network. IP security is merely a type of encryption while the security gateway is a firewall for protection against the outside world (Col. 6, L. 50-52). The IP Security and the security gateway are not disclosed as pointing from one network device to another. Nowhere does Barnes disclose or suggest "a set of Internet Security Association pointing from the second network element to the first network element".



In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). As described above, the combination of Havinis, Jokiahio and Barnes simply does not disclose or suggest the security association is a set of Internet Security Associations pointing from the second network element to the first network element. Therefore, claim 8 is patentable over the combination of Havinis Jokiahio and Barnes.

### 3. Claim 27

Claim 27 is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiahio in further view of Barnes. Claim 27 recites a data packet device being an integral part of a mobile station or being attachable to a mobile station comprising means for receiving information about a location information request and about a sender of a location information request from a mobile station and means for exchanging with a network element connected to a cellular network information about a security association, which points to the network element from the sender of the location information request.

Neither Havinis, Jokiahio nor Barnes discloses or suggests data packet device being an integral part of a mobile station or being attachable to a mobile station. Although this limitation is in the preamble of the claim, any terminology in the preamble that limits the structure of the claimed invention must be

treated as a claim limitation (M.P.E.P. § 2111.02). See, *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951) (A preamble reciting "An abrasive article" was deemed essential to point out the invention defined by claims to an article comprising abrasive grains and a hardened binder and the process of making it. The court stated "it is only by that phrase that it can be known that the subject matter defined by the claims is comprised as an abrasive article. Every union of substances capable *inter alia* of use as abrasive grains and a binder is not an 'abrasive article.'" Therefore, the preamble served to further define the structure of the article produced.); *Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1305, 51 USPQ2d 1161, 1165-66 (Fed. Cir. 1999); and *Jansen v. Rexall Sundown, Inc.*, 342 F.3d 1329, 1333, 68 USPQ2d 1154, 1158 (Fed. Cir. 2003).

The Examiner notes that Havinis fails to disclose that the second network element connects to a packet data network. Thus, there can not be any disclosure or suggestion in Havinis of a packet data device being an integral part of a mobile station or being attachable to a mobile station as claimed by Appellant as further evidenced by the figures of Havinis (Figs. 1, 2, 3, 4A, 5, 7 and 9).

Jokiaho also fails to disclose or suggest a packet data device being an integral part of a mobile station or being attachable to a mobile station. In particular, the data service center of Jokiaho is not the same as the packet data device of claim 27 as the data service center of Jokiaho is a computer located somewhere in the depths of a communications network and cannot be an integral part of a mobile station or attached to the

mobile station. In addition, the data service center (19) is disclosed in Jokiahho as being connected to a data service center (19) to the mobile services switching center (10), a base station controller or a base station (Col. 5, L. 2-5).

Furthermore, nowhere does Barnes disclose or suggest that a packet data device is an integral part of the mobile station or being attachable to the mobile station as called for in claim 27. The base station (16a, 16b) of Barnes is disclosed as being capable of establishing a wireless link with the mobile node (12) (Col. 7, L. 24-26), not as being an integral part of or attached to the mobile station.

In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). Claim 27 is patentable over Havinis, Jokiahho or Barnes, individually or in combination for at least the reason that these references fail to disclose or suggest a packet data device is an integral part of the mobile station or being attachable to the mobile station.

Furthermore, the examiner notes that the combination of Havinis and Jokiahho does not disclose or suggest the security association, which points to the network element from the sender of the location information request as called for in claim 27.

Although Barnes refers tangentially to "security associations" (i.e. IP Security at Col. 4, L. 13-18 and security gateway at Col. 4, L. 31-35), these are not the same as what is described and claimed by Appellant. The IP Security and the security gateway do not point to any one element of the network. IP security is merely a type of encryption while the security gateway is a firewall for protection against the outside world (Col. 6, L. 50-52). Neither the IP security nor the security gateway point to the network element from the sender of the location information request. Claim 27 specifically recites a security association which "points" to the network element from the sender of the location information request. Nowhere does Barnes disclose or suggest a security association that points to the network element from the sender of the location information request.

Thus, claim 27 is patentable over the combination of Havinis, Jokiahho and Barnes. Claims 28-32 are patentable by reason of their respective dependencies.

#### 4. Claim 28

Claim 28 is patentable under 35 U.S.C. 103(a) over Havinis in view of Jokiahho in further view of Barnes. Claim 28 recites means for establishing a second security association, which points to the device from the sender of the location information request and specifies at least data origin authentication. Neither Havinis, Jokiahho nor Barnes discloses these features.

As described above, Havinis notes that a positioning request is received [from an unknown party] by a serving mobile location center (Col. 4, L. 30-36) and does not disclose or suggest any

type of security association between the two. Havinis discloses a network that uses encryption algorithms. There are no dedicated security connections in Havinis nonetheless security associations that point from one network element to another network element. Furthermore, Havinis simply does not disclose or suggest "data origin authentication". Havinis merely discloses that when a positioning request for a particular mobile station is received by a serving mobile location center serving a cell within the public land mobile network that the mobile station is currently located in, the servicing mobile station must choose the optimum position method available (e.g. timing advance, time of arrival, angle of arrival, GPS, etc.) (Col. 4, L. 30-47).

Jokiaho, discloses a cellular radio system where the area covered by the system is divided into radio cells (Col. 4, L. 41 - 43; Fig. 1). Packets from all mobile stations within a specified area are routed to the data service center (Col. 5, L. 7 - 9). At the registration stage, there is also an exchange of ciphering keys which are used in the packets transmitted subsequently (Col. 7, L. 56-58). Jokiaho is concerned with reducing the amount of signalling for location management concerning packet transmission compared to location management concerning normal traffic and simply does not disclose or suggest "a second security association, which points to the device from the sender of the location information request" or "data origin authentication" as recited in claim 28. In addition, there is no location information request made in Jokiaho as the mobile station in Jokiaho initiates a location updating by transmitting a location updating request to the cellular radio network which causes the subscriber information

of the mobile station to be updated in the subscriber database of the cellular radio network (Col. 6, L. 54-63). This location updating request tells the cellular radio network that the mobile station is switching from one cell to another (Col. 7, l. 19-24).

Barnes tangentially refers to "security associations" (i.e. IP Security at Col. 4, L. 13-18 and security gateway at Col. 4, L. 31-35), but these are not the same as what is described and claimed by Appellant. The IP Security and the security gateway do not point to any one element of the network. IP security is merely a type of encryption while the security gateway is a firewall for protection against the outside world (Col. 6, L. 50-52). Neither the IP security nor the security gateway point to the device from the sender of the location information request. Claim 28 specifically recites means for establishing a second security association, which points to the device from the sender of the location information request. Furthermore, there is no disclosure or suggestion Barnes that a request from the "sender" specifies "at least data origin authentication" as recited in claim 28.

In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). As described above, the combination of Havinis, Jokiahho and Barnes fails to disclose

or suggest all the features of claim 28. Therefore, claim 28 is patentable over the combination of Havinis, Jokiaho and Barnes.

#### 4. Claim 29

Claim 29 is patentable under 35 U.S.C. 103(a) over Havinis, in view of Jokiaho and in further view of Barnes. Claim 29 recites means for requesting a network element of the cellular network to produce security documents relating to the device and to the sender of the information request for the establishment of the second security association. Neither Havinis, Jokiaho nor Barnes, individually or in combination disclose or suggest these features.

Havinis discloses a location deciphering key (Col. 5, L. 37-44) and a subscriber identification key (Col. 5, L. 50-58). However the location deciphering key does not relate to a "sender of the information request". The location deciphering key relates to the mobile station and its calculation of its position (Col. 5, L. 37-62). The subscriber identification key relates to a subscriber record (29) associated with the mobile station (Col. 5, L. 50-58). There is simply no disclosure or suggestion in Havinis of security documents relating to the device and to the sender of the information request as recited in claim 29.

Jokiaho also fails to disclose security documents relating to the device and to the sender of the information request. There is no information request made in Jokiaho. In Jokiaho, the mobile station initiates location updating by transmitting a location updating request to the cellular radio network (Col. 6, L. 54-55). This location updating request does not request information but rather tells the cellular radio network that the

mobile station is moving from one cell to another and to update subscriber information of the mobile station that is stored in the subscriber database of the cellular radio network (Col. 6, L. 60-63; Col. 7, L. 19-24).

Barnes discloses a network, system and method for merging a packet service such as GPRS with a mobile IP (Abstract). Nowhere does Barnes disclose or suggest security documents relating to the device and to the sender of the information request.

In order to establish a *prima facie* case of obviousness under 35 U.S.C. 103(a), there must be some suggestion or motivation, whether in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine reference teachings. There must also be a reasonable expectation of success, and the references, when combined, must teach or suggest all of the claim limitations (See M.P.E.P. § 2142). Claim 29 is patentable over the combination of Havinis, Jokiahho and Barnes because the references fail to disclose means for requesting a network element of the cellular network to produce security documents relating to the device and to the sender of the information request for the establishment of the second security association.



#### **VIII. CLAIM APPENDIX**

The texts of the claims involved in the appeal are:

1. A method (400) for processing location information, which is related to a certain mobile station in a cellular network, the method comprising the step of:

- a first network element, which is connected to the cellular network, receiving (401) a location information request (201) relating to the mobile station from a second network element, which is connected to a packet data network,
- requesting (404) from a third network element, which is connected to the packet data network, a security document relating to the second network element,
- initiating the establishment (406) of at least one security association, which security association specifies at least data origin authentication and points from the second network element to the first network element and which establishment involves use of information comprised in the security document,
- after successful establishment of said security association, authenticating (408) the data origin of the location service request, and

-if the data origin of the location service request is authenticated successfully, initiating (410) a location procedure relating to the mobile station in the cellular network.

2. A method according to claim 1, wherein the security document relating to the second network element is a public key certificate, which comprises an identifier specifying the second network element and a public key of the second network element and which is cryptographically signed by the third network element.

3. A method according to claim 1, further comprising the step of:

-requesting from the third network element a second security document relating to the first network element.

4. A method according to claim 3, wherein the security document comprises a first key, which is encrypted using a second key shared between the first network element and the third network element, and the second security document comprises the first key, which is encrypted using a third key shared between the second network element and the third network element.

5. A method according to claim 3, further comprising the step of:

-initiating the establishment of a second security association from the first network element to the second network element using at least information comprised in the second security document.

6. A method according to claim 5, wherein the security association is a set of Internet Security Associations pointing from the second network element to the first network element and the second security association is a second set of Internet Security Associations pointing from the first network element to the second network element.

7. A method according to claim 5, wherein the second security association specifies at least data encryption.

8. A method according to claim 1, wherein the security association is a set of Internet Security Associations pointing from the second network element to the first network element.

9. A method according to claim 1, further comprising the steps of:

-a third network element, which is connected to the packet data network, producing (404) said security document,

-establishing (406) at least one security association, which specifies at least data origin authentication and which points from the second network element to the first network

element, using at least information comprised in the security document, and

- after the establishment of said security association, authenticating (408) the data origin of the location service request, and

- carrying out (701) a location procedure relating to the mobile station in the cellular network.

10. A method according to claim 9, further comprising the step of:

- transmitting (707, 713) location information relating to the mobile station to the second network element.

11. A method according to claim 10, wherein the location information relating to the mobile station is transmitted to the second network element from the first network element.

12. A method according to claim 11, further comprising the steps of:

- the third network element producing a second security document relating to the first network element, and

- establishing a second security association, which specifies at least data encryption and points from the first network

element to the second network element, using at least the information specified in the second security document.

13. A method according to claim 10, further comprising the step of:

- before transmitting the location information to the second network element, establishing (708) a third security association, which specifies at least data origin authentication and points from the second network element to a packet data device, which is either connected to the mobile station or is an integral part of the mobile station.

14. A method according to claim 10, wherein the location information relating to the mobile station is transmitted from a device, which is either connected to the mobile station or is an integral part of the mobile station.

15. A method according to claim 14, further comprising the step of:

- before transmitting the location information to the second network element, establishing (708) a third security association, which specifies at least data origin authentication and points from the second network element to a packet data device, which is either connected to the mobile station or an integral part of the mobile station.

16. A method according to claim 15, further comprising the step of:

- before transmission of location information, establishing (710) a fourth security association, which specifies at least data encryption and which points to the second network element from said packet data device.

17. A method according to claim 14, further comprising the steps of:

- the mobile station receiving (702) a notification relating to the location procedure relating to the mobile station, and
- the mobile station informing (703) said packet data device about the notification.

18. A method according to claim 1, wherein the first network element is a network element of a GPRS network.

19. A method according to claim 18, wherein the first network element is a Gateway Mobile Location Center.

20. A method according to claim 1, wherein the first network element is a network element of a UMTS network.

21. A network element (900) of a cellular network, the network element comprising

- means (910) for receiving from a packet data network a location information request relating to a certain mobile station,
- means (920) for initiating a location procedure in the cellular network,
- means (930) for establishing security associations pointing to the network element from a network element of the packet data network,
- means (931) for performing security functions as specified by the security associations on data it receives from the packet data network,
- means (932) which are arranged to determine, if there is an existing security association pointing to the network element from a sender of a location information request, and
- means (933) for initiating security association establishment, which are arranged to establish a security association if there does not exist a security association, which points towards the network element from the sender of a location information request.

22. A network element according to claim 21, further comprising

- means (940) for receiving from a device reachable via the cellular network a request about a security association, which points to the network element from a certain network element of the packet data network,
- means (932) for determining whether a requested security association exists, and
- means (940) for transmitting information about the requested security association to the device.

23. A network element according to claim 21, further comprising

- means (943) for receiving a request to produce security documents relating to the device and to the sender of a location information request, and
- means (944) for producing a first security document relating to the device and a second security document relating to the sender of the location information request.

24. A network element according to claim 21, wherein it is a network element of a GPRS network.

25. A network element according to claim 24, wherein it is a Gateway Mobile Location Center.



26. A network element according to claim 21, wherein it is a network element of a UMTS network.

27. A packet data device (950) being an integral part of a mobile station or being attachable to a mobile station, comprising

- means (960) for receiving information about a location information request and about a sender of a location information request from a mobile station and
- means (970) for exchanging with a network element connected to a cellular network information about a security association, which points to the network element from the sender of the location information request.

28. A device according to claim 27, further comprising means (980) for establishing a second security association, which points to the device from the sender of the location information request and specifies at least data origin authentication.

29. A device according to claim 28, further comprising means (980) for requesting a network element of the cellular network to produce security documents relating to the device and to the sender of the information request for the establishment of the second security association.

30. A device according to claim 27, further comprising means (990) for transmitting to the mobile station a permission to send location information to the sender of the location information request, which means are arranged to transmit the permission when there is said security association.

31. A device according to claim 27, further comprising means for locating itself.

32. A device according to claim 31, comprising a Global Positioning System receiver.

33. A mobile station (901), comprising

- means for receiving a notification from a cellular network about the location information request,
- means for responding to the cellular network with a notification response, and
- means for notifying a packet data device, which is either an integral part of the mobile station or attached to the mobile station, about the location information request.

34. A mobile station according to claim 33, wherein the means for responding to the cellular network are arranged to be initiated by a permission sent by the packet data device.

**IX. EVIDENCE APPENDIX**

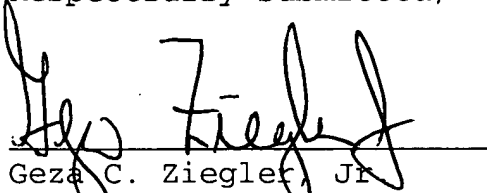
Not Applicable.

**X. RELATED PROCEEDINGS APPENDIX**

Not Applicable.

A check in the amount of \$500 is enclosed herewith for the appeal brief fee. The Commissioner is hereby authorized to charge payment for any additional fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,



Geza C. Ziegler, Jr.  
Reg. No.: 44,004

20 Jan 2006  
Date

Perman & Green, LLP  
425 Post Road  
Fairfield, CT 06824  
(203) 259-1800  
Customer No.: 2512

#### **CERTIFICATE OF MAILING**

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date indicated below as first class mail in an envelope addressed to the Board of Patent Appeals and Interferences, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450,

Date: 1-20-2006

Person Making Deposit

Signature: Jessica Ree